REPORT ON PRIOR HEARING AND GENERAL CONSULTATION PROCEDURE HELD REGARDING THE DRAFT DECISION ON:

- **the circumstances, format and procedures applicable to the requirements of reporting, by companies that provide public communications networks or publicly available electronic communication services, of security breaches or losses of integrity with significant impact on the operation of networks and services (Paragraph 2 of articles 54-C and 54-B of the LCE);**
- **the conditions by which ICP-ANACOM considers that there is public interest in public disclosure, by companies that provide public communications networks or publicly available electronic communication services, of security breaches or losses of integrity with significant impact on the operation of networks and services (point b) of article 54-E of the LCE)**

A - BACKGROUND

By determination of its Management Board, on 22 December 2011, Autoridade Nacional de Comunicações (ICP-ANACOM) approved a Draft Decision on:

- the circumstances, format and procedures applicable to the requirements of reporting, by companies that provide public communications networks or publicly available electronic communication services, of security breaches or losses of integrity with significant impact on the operation of networks and services (Paragraph 2 of articles 54C and of the LCE);

- The conditions by which ICP-ANACOM considers that there is public interest in public disclosure, by companies that provide public communications networks or publicly available electronic communication services, of security breaches or losses of integrity with significant impact on the operation of networks and services (point b) of article 54-E of the LCE)

It was also decided to submit this Draft Decision to the prior hearing of interested parties, pursuant to articles 100 and 101 of the Código do Procedimento Administrativo (Administrative Proceeding Code), as well as to the general consultation procedure laid down in article 8 thereof and in paragraph 4 of article 54-C of Lei das Comunicações Eletrónicas (Electronic Communications Law - "LCE" in the present document - as approved by Law no. 5/2004 of 10 February and as subsequently amended by Decree-Law no. 176/2007 of 8 May, by Law no. 35/2008 of 28 July, by Decree-Law no. 123/2009 of 21 May, by Decree-Law no. 258/2009 of 25 September, Law no. 51/2011 of 13 September, Law no. 10/2013 of 28 January and by Law no. 42/2013 of 3 July). Interested parties were granted a period of 20 working days, under both procedures, in which to comment, whereby comments were to be submitted no later than 27 January 2012.

Under this procedure, timely contributions were received from:

- undertakings providing public communications networks or publicly available electronic communications services (*"companies"* in the present document), AT&T/COLT/Verizon Business in joint response, Cabovisão, CTT, Grupo ONI (Onitelecom, Knewon, and F300), Optimus, Grupo PT (Portugal Telecom, S.G.P.S., S.A., PT Comunicações, S.A., and TMN - Telecomunicações Móveis Nacionais,

S.A.), Vodafone and ZON (ZON TV CABO, ZON TV CABO MADEIRENSE and ZON TV CABO AÇOREANA), as well as from APRITEL - Associação dos Operadores de Telecomunicações (Association of Telecommunications Operators);

- consumer associations: ACOP - Associação de Consumidores de Portugal (Portugal Consumer Association) and UGC - União Geral de Consumidores (General Union of Consumers); and
- public bodies: DGC - Direção Geral do Consumidor (Directorate General for the Consumer) and Secretaria Regional da Educação e Recursos Humanos do Governo Regional da Madeira (Regional Education and Human Resources Secretariat of the Regional Government of Madeira).

An additional contribution was received from DECO - Associação Portuguesa para a Defesa do Consumidor (Portuguese Association for Consumer Protection), together with a revised version of the contribution submitted by Optimus, but since both were received subsequent to the stipulated deadline, these were not considered in this report.

With the consultation process concluded, it is now important to prepare the resulting report and publish the responses received, excluding items which were considered confidential (these confidential items were taken fully into account and not just in the content transposed or cited in the summary included in the present report).

This report therefore presents the summary of responses submitted to the public consultation and positions taken by ICP-ANACOM on the issues raised, and sets out the reasoning giving basis to the options taken in the final decision.

First, however, and with regard to the suggestion put by Grupo PT as regards the *"establishment of a working group comprising all stakeholders, in order to ensure both the definition of security incidents to be reported and the definition of proportionate measures which are in line with the practical reality of the sector and which take the criticality of the services into account"*, it can be stated, from the outset, that ICP-ANACOM is of the position that, in the current framework, this suggestion cannot be accepted, given that:

a) Pursuant paragraph 2 of article 54-C of the LCE, it is incumbent upon ICP-ANACOM to approve measures defining the circumstances, format and procedures applicable to notification requirements concerning breach of security or loss of integrity of

networks; and

b) Pursuant to 4 paragraph of the same Article, the adoption of implementing measures referred to in paragraphs 1 and 2 is subject to the general consultation procedure provided for in article 8 of the LCE, so that the law deems this the appropriate procedure to ensure that stakeholder contributions are taken on board with a view to improving the content of this decision.

In any case, subsequent to the entry into force of this Decision, the Authority remains available to receive and examine any contributions that might lead to its efficient implementation.

Finally, it should also be noted that after the public consultation, ICP-ANACOM has obtained access to statistical data on the occurrences of crimes of theft and damage to infrastructure used for the provision of electronic communications networks and services in the years 2010 and 2011.

Having examined the facts in order to determine their relevance to the present decision-making process, ICP-ANACOM concluded that the data added no new elements of relevance to the present decision.

B - GENERAL CONSIDERATIONS

1. By the companies and APRITEL:

- **AT&T, COLT and Verizon Business**, in a joint response given in English[1], refer to their specificity as companies limited only to the delivery of pan-European and global services to large corporate clients; as such, they emphasise the need for implementation that is identical in all Member States of the European Union (EU), with a view to the benefits arising from close coordination across the EU, the accomplishment of which would be desirable even without formal harmonization measures.

  In line with the above, these companies consider that ICP-ANACOM should follow the document[2] published by ENISA[3] on 10.12.2011, while granting that reporting of companies to National Regulatory Authorities (NRAs) is outside the scope of that document.
- **Cabovisão** *"welcomes ICP-ANACOM's initiative to define the circumstances, format and procedures applicable to the requirement to report breaches of security and network integrity, (...) considering this to be the only way to ensure consistency in approach to this issue (...) "*.

  The company also states that *"it gives paramount importance to the protection of integrity and security of its electronic communications networks and services, as evident from the large investments it has made in this area (...) "*.

  However, notwithstanding the above, Cabovisão takes the view that *"it is essential that ICP-ANACOM looks again at certain aspects of the Draft Decision with regard to the reporting of security incidents (Draft Decision I), otherwise it is in danger of adopting an overly demanding position, unmatched by the positions taken by ENISA and OFCOM (...) "*.
- **CTT** states that, in its capacity as virtual mobile network operator, *"all the electronic communications services which it provides are supported over TMN's mobile network, whereby TMN is the operator responsible for the security and integrity of*

[1] Whereby any discrepancies are safeguarded as may occur in the present document, arising in our translation and respective position, as regard to the what these companies would wish to have expressed in English.

[2] Available at http://www.enisa.europa.eu/act/res/reporting-incidents/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting .

[3] *European Network and Information Security Agency*.

services provided by CTT to their customers" and insofar as the Draft Decision *"makes providers such as CTT, as operators without network infrastructure, subject to obligations of security and integrity of the network where their services are supported"*, the company would be required to subcontract additional services under its contract with TMN to comply with such obligations.

CTT also takes the view *"that given the small size of CTT (...), the accomplishment of network security obligations will entail significant administrative costs in its activity, having a direct impact on end-consumers, their customers"*; this is of great concern to CTT, so that *"ICP-ANACOM should establish mechanisms that reflect the reality of operators which do not possess networks (...), limiting the obligation now under consultation to operators in possession of networks as the only operators with the means to detect and identify incidents security occurring on their network "*.

- **Grupo ONI** considers that the Draft Decision represents *"an important step for the operational implementation of the provisions already transposed into National Legislation, and so welcomes this initiative of ICP-ANACOM. However, the provisions of the Draft Decision require important adjustments to bring them into line with the reality of the market, need to take the real usefulness of information to be provided into account, must not contribute to an increased level of risk and not cause the public undue alarm, nor contribute to giving the sector an undeserved poor image"*.
- **Optimus** agrees with ICP-ANACOM as to the relevance given to security and integrity of networks and services, and therefore *"has implemented various internal assurance and prevention procedures with regard to security incidents, particularly related to interruption of service (...) embodied at a number of levels"*.

  The company claims that, in its opinion, the Draft Decision provisions relating to *"proposed (demanding) reporting obligations"* do not concur with the requirements set out in article 5 of the LCE, so that by adopting the parameters set out therein, *"ICP-ANACOM could receive a large number notifications from operators arising naturally from the effects had by to network management activities which are subject to equipment and service failures, but which are not really significant from a national perspective, or for the public"*.

  Optimus also mentions the need to clarify how ICP-ANACOM will intervene during a security incident in terms of reporting deadlines.

  It adds that *"The scope of services and parameters to be considered for notification should reflect circumstances of failure that are truly fundamental and critical and*

which affect national security or represent emergency situations", and stresses *"that in assessing the proportionality and reasonableness of the measures to be imposed, ICP-ANACOM cannot fail to consider the costs of implementation and operation. The obligations that will be defined cannot entail weighty investment or a considerable increase in administrative costs for operators without clear benefits for the market in general and users in particular. This aspect is particularly relevant in the current macroeconomic and financial environment, as characterized by declining economic activity and difficulties in accessing finance. "*.

- **Grupo PT** reveals the "*ex novo" character* of the issues under consideration and the importance it attaches to security, which has led it to undertake significant investments in this area and to establish a Security Committee and a Privacy and Personal Data Protection Committee.

  Given the importance which Grupo PT gives to all matters relating to Security and Integrity of Networks and Services, *"it is pleased to witness the enshrinement, at a legal and regulatory level, of measures which will certainly contribute to strengthening the focus of operators on the adoption of measures to ensure minimal risk in terms of network security and integrity. Additionally, the clear benefits that such activities will have for the sector as a whole should not be underplayed, since it will bring clear benefits for all stakeholders"*.

  However, the Group express disagreement with certain aspects of the Draft Decision, such as the establishment of *"conditions (triggering thresholds) which are more stringent than those set out, for example, by OFCOM, both with regard to the duration of the incident to be considered for reporting purposes, and with regard to reporting deadlines, as well as with regard to the number of notifications which may occur and their content, among other things"*; it cites the need to *"refer to the existing benchmark and to the rationale inherent to the reporting obligation - ensuring that only really significant incidents are reported - to assess the real benefits that can be derived from notifications"*.

  It held that, prior to the definition of notification procedures, technical measures should be implemented as deemed appropriate in light of article 54-A of the LCE, setting out a position in line with the rationale governing the reporting of personal data breaches to subscribers, as in the Privacy Directive.

  It further refers to: the need for a specific definition of *"security incident"*, the possible disproportionate nature of costs incurred in terms of the objectives to be achieved (invoking OFCOM's document once again), the need to limit the services covered

according to their criticality, *"as, for example, set out by ENISA in its draft communication template"*, and the differences which, in its opinion, should exist between MNOs and MVNOs.

The Group considers that the Draft Decision, in terms of reporting to ICP-ANACOM, *"implies an overly bureaucratic reporting scheme, which should be made more flexible and streamlined"*.

As regards the provision of information to users, it warns *"security incidents may be used by the media, especially those with a more sensationalist editorial line"*, and recalls that ICP-ANACOM has an obligation under law to assess the public interest in the disclosure of security incidents under the terms of the law, arguing that such disclosure should be made on a case by case basis.

Finally, it expresses disagreement as regards the implementation period of 30 days proposed by ICP-ANACOM, and suggests the creation of a working group incorporating all stakeholders, in which it is willing to participate, based on its view that any decision made by the Regulator in relation to the matter under consideration should result from efforts of coordination between ICP-ANACOM and the companies providing electronic communications networks and services.

- ***"Vodafone** acknowledges the importance of ensuring constant security and integrity of electronic communications networks and services (...) having, naturally, implemented the mechanisms necessary for preventing and managing risks arising from security incidents. "*.

  Vodafone considers that, in the Draft Decision, ICP-ANACOM employs criteria which are not in line with those used by ENISA, such as reporting incidents with a duration of less than one (1) hour, as well as imposing *"a set of additional criteria, also not covered in the ENISA guidelines, and mandatory deadlines for incident reporting which are clearly demanding, making the reporting procedure more complex and demanding from a technical and administrative point of view, and therefore more costly for operator "*.

  "As such, if we consider the deviation adopted by ICP-ANACOM, as lacking clear justification, in the definition of the type of incidents to be reported in terms of the criteria defined at European level, the rationale underlying the reporting requirements, as well as the onus that such an approach would entail for operators, we cannot but conclude that the measures imposed in the Draft Decision are disproportionate".

  As regards the public interest in disclosure to the public of a security incident,

Vodafone believes that assessment should be undertaken on a case by case basis and that use of the same criteria as used for notification to the regulator is inappropriate and unjustified; this position represents Vodafone's most significant reservations, due to the fact that it could be established that a reported incident had no significant impact and therefore its disclosure to the public within the prescribed period is not warranted.

Finally, given what it claims is the new nature of the subject and the insufficiency of the 30-day implementation period provided for in the Draft Decision, the company calls for the establishment of a period of not less than 6 months.

- *"**ZON**, following the best practices in the industry, has invested heavily in internal control processes aimed at assurance and preventing security incidents and has participated at various levels in specialized forums on monitoring and researching security policy practices"*; the company *"is particularly committed to preventing and combating security breaches and losses of integrity that may impact electronic communications networks and services"*.

  ZON considers that the Draft Decision *"presents a model that entails a set of obligations which greatly exceeds those recommended in Directive 2002/21/EC (Framework Directive), as amended by Directive 2009/140/EC, and also exceed those defined by ENISA in its Technical Guideline on Incident Reporting"; the Draft Decision sets out "triggering thresholds"* with a minimum duration that are much shorter than as defined by the ENISA document and even when compared to the rules of another NRA (OFCOM), *"the reporting deadlines"* and *"the number of notifications required and their content (two mandatory notifications and a third possibly required according to a subjective criterion)"*.

  As regards the issue of public disclosure (Annex B of the Draft Decision), ZON considers that it should be defined on a case by case basis, as *" results from the new paragraph 3 of article 13-A of Directive 2002/21/EC, which the LCE transposed into national law"*.

  ZON considers that a minimum implementation period of six months should be granted since *"the present Draft Decision will be innovative, with an absence of any information that may be obtained from other NRAs about the pitfalls of implementing such a regulation"*, and concludes that *"the reporting at issue here should not impose a new set of obligations without the respective regulatory impact analysis being performed and shared with the stakeholders, serving to assess the impacts resulting therefrom"*.

- **APRITEL** begins by highlighting the references made by ICP-ANACOM in the Draft Decision as to the novel nature of the subject and as to the provisions of the LCE being *"Sufficiently precise to enable companies to further develop their work".*

  APRITEL then stated that *"APRITEL's members already attach the utmost importance to the issue of security and integrity of their electronic communications networks and services and have implemented a range of internal procedures of assurance and prevention of security incidents, promoting and participating in mechanisms of sector cooperation, (...) the priority given to this issue by operators is demonstrated by the substantial investment that the sector as a whole has made in the implementation of measures to guarantee security"*.

  Understanding the rationale of the Draft Decision, APRITEL considers *"that any decision taken in this context, as regards the type of situations that should be subject to reporting, should be guided by proportionality and flexibility of approach, taking into particular account the onus imposed on the companies (...) and the ultimate aim of such measures"*; it takes the view that the *"ICP-ANACOM has ended up adopting an overly demanding position for the sector (....), which is without parallel in the positions adopted by ENISA or other national regulatory authorities, such as the British authority OFCOM, (...) including as regards incident duration, notification deadlines, the number of notifications required and their content"*.

  They emphasise this point, stating that, *"in practice, these requirements correspond to obligations which fall on the companies, entailing significant administrative costs, and which are clearly disproportionate in terms of the efforts required of operators, existing benchmarks, the rationale of the notification obligation - to ensure that only incidents which are really significant are reported - the usefulness that ICP-ANACOM might derive from the high volume of notifications which it is likely to receive in the event that the criteria remain defined as they are, and, above all - it underlines - the potential fines provided for in the LCE for breach of the obligation to notify the NRA, which can reach one million euros"*.

  "With respect to the Draft Decision and as regards the conditions in which ICP-ANACOM considers that there is a public interest in public disclosure, APRITEL considers the Regulator's option to be inappropriate, in light for example, of the total absence of guidelines from ENISA or OFCOM in this matter", considering that ICP-ANACOM should determine *"which incidents warrant public disclosure on a case by case basis, and based on the specific characteristics of the respective case to*

determine whether or not there is public interest in widespread disclosure"; this view results from its interpretation of the provisions of the LCE (Article 54-E) and Directive 2002/21/EC (paragraph 3 of article 13-A).

APRITEL does not then support disclosure to the public *"of all security incidents that are reportable under the First Draft Decision (Annex A of the consultation)"*, considering that, *"beyond being petty and without concrete legal basis, such disclosure may cause alarm among consumers."*.

APRITEL is of the view that ICP-ANACOM needs to undertake a *"review of the Draft Decision in light of the concerns of the sector, in order to provide a more flexible approach and adapt it to the reality of the companies affected, which is described in the following chapters."*.

Finally, APRITEL express expresses *"the deep concern of its members as to the implementation deadline set by ANACOM (...), which should be in no event less than 6 months for the implementation of the procedures after the publication of the final decision"*.

2. **By consumer protection associations:**

- **ACOP** expressed its agreement with the draft.
- **UGC** issued *"a favourable opinion of the draft clauses, with the view that they will strengthen the right of consumers to information, specifically as a result of the provisions of Annex B"* and considered *"recognition of the need to ensure the security and integrity of publicly available electronic communication networks and services very positively, given the importance for all citizens".*

3. **By the public administration:**

- *"**DGC** considers this initiative to be very important for consumers, not just by requiring a qualitative effort from operators as regards investment in security and risk management, but likewise insofar as it creates conditions for increased visibility of situations with lapses in quality of service, thereby enabling a new comparative indicator: reliability of the service provider"*(...), taking the view that *"the Draft Decisions should be adopted"*.

  DGC asks *"whether consideration had been given to the effect that the costs of implementing and managing the systems might have in increasing the price of*

services. Moreover, the different media and technological environments (ADSL, fibre, copper, for example) reflect different capacities in terms of action and problem resolution times, which is not provided for in the Draft Decision and is not referenced in the text".

- **GRM** *"Highlights the fact that the geographical and political-administrative realities of the autonomous regions had been into account"*, as regards the reporting obligation, set out in Annex A to the Draft Decision.

4. Position of ICP-ANACOM

Without prejudice to the positions that ICP-ANACOM takes on the specific matters of Annexes A and B to the Draft Decision, at this point we cannot but set out our position on some points made above, which, in our view, also denote the diligence of ICP-ANACOM's approach in the Draft Decision as to the principles to be applied and as to how its powers, as set out in Article 5 of the LCE, would be exercised:

1) ICP-ANACOM welcomes the importance that companies providing electronic communications networks and services (companies) give to the issue of security and integrity of their networks and services, with effective expression in the investments they claim to have already undertaken, including in the implementation of assurance procedures and the prevention of security incidents.

   This matches ICP-ANACOM's expectation as to the result of the activity it has undertaken in the past, as referred to in the Draft Decision, in order to *" to promote a security culture in the sector and, at the same time as giving warning and changing the mindset, highlighting the need for, among other things, companies providing public communications networks or publicly available electronic communications services to acquire the means to respond in a timely manner to today's new challenges of security and integrity of networks and services"*.

2) As regards Grupo PT's position on the need for a prior definition of technical and security measures, pursuant to article 54-A and paragraph 1 of article 54-C of the LCE, and despite this area being relatively recent, as revealed in the contributions sent to us and in the previous point, it is reiterated that, as was set out in the Draft Decision, *"the provisions of the LCE are clear and precise, so that companies and ICP-ANACOM may develop their work in this area in the short-term (...) "* (emphasis added).

   Indeed, and contrary to Grupo PT's argument and as, in general, is considered to be in line with contributions from the companies on subject, ICP-ANACOM holds it would be premature to define technical measures as referred to in the provisions of Article 54-A of the LCE; instead, the companies would be better positioned, initially, to assess the relative risks to their networks and services.

   Furthermore, the provisions of paragraph 2 of Article 54-C of the LCE are in keeping

with this view - *"...the NRA is entitled to approve and impose technical implementing measures ..."* (emphasis added) - as compared to the provisions of paragraph 1 of this article - *"...it is incumbent on the NRA to approve measures defining the circumstances, format and procedures applicable to notification requirements concerning breach of security or loss of integrity of networks"* (emphasis added).

Exercise of the authority provided for in paragraph 1 of article 54-C of the LCE requires, in ICP-ANACOM's opinion, continuous monitoring of security breaches or losses of integrity reported to ICP-ANACOM and an assessment of the information conveyed to it in this respect, including a description of the measures which companies have implemented; ICP-ANACOM will not be in a position to consider a possible imposition of technical implementing measures, until after this assessment has been performed. Naturally, this does not exempt the clear and precise responsibility conferred on companies by the provisions of Article 54-A of the LCE.

3) The position of Grupo PT, in the sense that the reporting regime laid down in article 4 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("Privacy Directive") would, as regards the public disclosure of breaches of security or loss of integrity, be more in line with the ultimate goals underlying network security regulation, avoiding situations of general unjustified alarmism, cannot have ICP-ANACOM's agreement.

   Firstly, the unequivocal difference, assumed in the review of the EU regulatory framework, must be taken into account, including:

   a) On the one hand, the regime of public disclosure of breaches of security or losses of integrity, as provided for in the final part of point 2 of paragraph 3 of article 13-A of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ("Framework Directive") and, in Portugal, in point b) of Article 54 of the LCE; and
   b) On the other hand, the regime governing the reporting of breaches of personal data, as provided for in point 2 et seq. of paragraph 3 of article 4 of the Privacy Directive and, in Portugal, in paragraphs 2 et seq. of article 3-A of Law no. 41/2004 of 18 August, as amended and republished by Law no. 46/2012 of 29 August.

   Secondly, consideration is given in the position expressed in section 10 below,

pointing to the same approximation of the Finnish regulator.

4) The reference by APRITEL that ICP-ANACOM should be more flexible in its approach to this matter finds possible echo, in our opinion, in the approach taken by this Authority.

   Indeed, intent on a possible future and continuous improvement resulting from the perception and analysis entailed in its development, and as had also been mentioned in the Draft Decision, ICP-ANACOM made some adjustments in this document over the Draft Decision, in view of the comments received, which in our view reflects the flexibility of the approach taken.

5) References by the majority of companies and by APRITEL to the need for harmonization, in the European market, of the measures adopted by the various regulators with the measures advocated in the document "*Technical Guideline on Reporting Incidents*", published by ENISA - European Network and Information Security Agency, *to benchmark* with other regulators, especially with OFCOM[4], and the measures advocated (all of which we were aware of in time, and meriting our attention), gives basis to our position as follows:

   a) Bearing in mind that, pursuant to paragraph 4 of article 13-A of the Framework Directive, *"the Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical implementing measures with a view to harmonising the measures referred to in paragraphs 1, 2 and 3 (...) "*, it is noted, first and foremost, that, to date, the European Commission has not approved any technical implementing measures in this area, which fact, however, does not exempt NRAs from exercising their powers within national legal frameworks;

   b) The document "*Technical Guideline on Reporting Incidents*", sponsored[5] by ENISA, which was taken into consideration in this process, does not constitute the opinion referenced in paragraph 4 of article 13-A of the Framework Directive, and is not binding in itself. It also has a distinct objective and context, since it does not refer to company notifications to the NRAs, nor at this time, all electronic communications networks and services; its primary focus is at European level, i.e., it does not address the different

[4] Document available at: http://stakeholders.ofcom.org.uk/binaries/telecoms/policy/security-resilience/guidance.pdf.

[5] Indeed the document does not constitute (as explicitly stated) any position or opinion of ENISA.

national realities which it each NRA is bound to examine, taking into account the legislation adopted by the respective Member State.

c) Incidentally this aspect of the national reality of each Member State seems important to us, and we consider the position of OFCOM and their document as a good example.

OFCOM's approach stems from a very different reality, including in terms of the industrial level of the sector in the country, in terms of the incumbent bodies and mechanisms/agreements with respect to security/emergency matters, and in terms of adopted codes of conduct, etc. as have allowed to OFCOM indicate, for example, that companies are to report security incidents which they are aware of being reported in the media[6], and not requiring (although not totally and for the moment[7]) notification of security incidents outside of normal office hours due to the existence of NEAT (National Emergency Alert for Telecoms), of which it is part; as is also the case in Sweden with NTCG (National Telecommunications Crisis Management Coordination Group) chaired by PTS (Sweden's NRA).

It should be noted, with reference to OFCOM's proposals, with which we somewhat concur, as regards repeated incidents, these were generally opposed by the companies.

It is also noted that OFCOM has taken into account in the definition of the services and thresholds, in a very specific interpretation, the proposals of CPNI[8] (3.50 *"We have developed a set of service specific reporting thresholds to be used as guidance when considering whether a breach of security or loss of availability has 'had a significant impact on the operation' of a network or service, based on proposals from CPNI"*).

d) It is also important to be aware, for example, of the approaches taken by the Finnish (FICORA) and Swedish (PTS) regulators to the matters under consideration, from the outset, as bodies which have long been devoting

---

[6] 3.49 *"Any incidents that CPs are aware of being reported in the media (local, national or trade news sources)".*

[7] For major incidents notifications are no longer considered in real time (3.43 *"CPs may wish to consider submitting reports in real time"*) and retain the option of revising this guideline (3.*40 "we are not planning to monitor received reports outside of normal office hours, although this will be reviewed if required following the introduction of the reporting arrangements"*).

[8] *Centre for the Protection of National Infrastructure*.

extensive human and financial resources to the area of secure communications; these are available respectively at: http://www.ficora.fi/attachments/englantiav/64u7tHKEx/Viestintavirasto57A2012MEN.pdf and http://www.pts.se/upload/Foreskrifter/Tele/ptsfs-2012_2-avbrott-och-storningar.pdf (in Swedish only), whereas note is made, from the outset, of the question of information to be provided to users, as set out in the document from FICORA (as entered into force on 1 February 2012) , and the thresholds defined in the document from PTS (as entered into force on 1 April 2012) .

Note is also made of the approach taken by the Lithuanian regulator RRT (www.rrt.lt), available at https://www.cert.lt/en/legal_acts.html, which differs from the others.

6) Optimus argued for the need to clarify ICP-ANACOM's role during a security incident in terms of the established reporting deadlines; in this respect, for a thorough pursuit of its duties and the proper exercise of its powers in terms of security and integrity, ICP-ANACOM considers it necessary to have access to information that enables real-time monitoring of security breaches and losses of integrity, and not only their subsequent analysis.

   In fact and considering that:

   a) Pursuant to paragraph a) of article 54-E of the LCE, it is incumbent upon ICP-ANACOM to inform the national regulatory authorities of other Member States and the European Network and Information Security Agency (ENISA) where this is deemed to be justified on account of the scale or seriousness of the breach of security or loss of integrity notified pursuant to article 54-B of the LCE;

   b) Pursuant to paragraph b) of Article 54-E of the LCE, it is incumbent upon ICP-ANACOM to inform the public, by the most appropriate means, of any breach of security or loss of integrity or to require undertakings that provide public communications networks or publicly available electronic communications services to do so, where it determines that disclosure of the breach is in the public interest;

   c) Under the terms of paragraph 1 of article 54-G of the LCE, ICP-ANACOM shall, for the purpose of articles 54-A and 54-B, and in the scope of technical implementing measures and additional requirements adopted, have the

power to issue binding instructions to undertakings providing public communications networks or publicly available electronic communications services, including those regarding time limits for implementation;

The position is taken that it is necessary for ICP-ANACOM to be provided with the means necessary for constant and real-time monitoring of security breaches or losses of integrity (situation awareness) with a view that, where appropriate, ICP-ANACOM may, in due course, inform the public, the national regulatory authorities of other Member States and ENISA, as well as formulate response actions and, where appropriate, issue binding instructions.

In this sense, and in general, we recall recital 44 of Directive 2009/140/EC of the European Parliament and of the Council of 25 November, which states that *"national regulatory authorities should therefore ensure that the integrity and security of public communi-cations networks are maintained"*.

Finally, the assignments conferred upon ICP-ANACOM by article 2-A of the LCE on security and emergency issues are also relevant, as well as its future assignments in the area of civil emergency planning, resulting from ICP-ANACOM inheriting the duties and powers of the Comissão de Planeamento de Emergência das Comunicações (Emergency Communications Planning Committee).

7) As regards the applicability of this decision to MVNO[9], a question raised by CTT and Grupo PT in light of the cited absence of network infrastructure, it is made clear that:
   a) In accordance with Article 54-B of LCE, undertakings providing (i) public communications networks or (ii) publicly available electronic communications services shall notify ICP-ANACOM of a breach of security or loss of integrity with a significant impact on the operation of networks or services.
   b) According to the explanation already provided by ICP-ANACOM on this matter and taking into account the definitions in article 3 of the LCE, an MVNO is a provider of electronic communications services, which may also, depending on the adopted business model and whether it controls elements of the transmission system and network infrastructure, provide electronic communications networks; and
   c) In this context and insofar as it offers publicly available electronic communication services, an MVNO is accordingly bound to notify ICP-ANACOM as to any breaches of security or loss of integrity with significant

[9] *Mobile Virtual Network Operator*

impact on the operation of its services and also, as is the case, on the operation of their public communications networks.

8) The need to define the concept of *"security incident"*, as claimed by Grupo PT and Cabovisão merits the following comments and view:
   a) In the establishment of the obligation of companies to report security incidents to the NRA, the first point of paragraph 3 of article 13-A of the Framework Directive and, in Portugal, article 54-B of the LCE adopted without any further embodiment, the concept of *"Breach of security or loss of integrity"*;
   b) This lack of definition, at Community and national level, of breach of security or loss of integrity is not, in our view, the result of any omission but fully intentional; one of the reasons, if not the main reason, why this subject of security and integrity of networks and services is brought under regulatory policy is, in particular, the need for regulatory authorities to know which causes are seriously disrupting the functioning of the services provided by electronic communications networks and services, alongside the recognition that knowledge of these causes has, so far, remained internal to companies;
   c) The solution adopted at the level of the ENISA and OFCOM documents is, first, to recognize this lack of knowledge and then, try to address the concepts of *"Breach of security or loss of integrity"* with another concept which covers both, whereby it was decided to use the term *"security incident"*;
   d) It is not important that the definition of security incident does not correspond to a precise and limited concept, since what matters is that, having determined that an event, whatever its nature, caused the occurrence of a serious disturbance in the functioning of networks and services, with a significant impact on the continuity of operation, pursuant to paragraph 2 of Section I of Annex A and in accordance with the conditions and rules set out in paragraphs 3 et seq. of the same Section I, this event is reported and, where appropriate, disclosed to the public;
   e) The usefulness of the notification is derived not only at the moment of informing the NRA, but also later in analysing the causes that led to the incident and the measures taken. As such, we have a regime which aims, on the one hand, to increase transparency of what is happening on the network or service and, on the other, to introduce a system of continuous improvement in the security and integrity of electronic communications

networks and services;

f) As regards the ENISA and OFCOM documents, the first uses a concept with a character of non-formal technical guidance, and the second a concept of guidance and interpretation;

g) It should be noted that, in its regulations, neither FICORA nor PTS defined such concepts;

h) In this sense and to ensure greater clarity, it was decided to remove the aggregator term of "security incident" from the final version of the decision and use the definition adopted, and not implemented, by Article 54-B of the LCE: "breach of security or loss of integrity".

9) The majority of companies argued for the need to define the scope of the networks and services covered based on their criticality, with some of the companies citing, for this purpose, the examples of the positions taken by ENISA and OFCOM. In this regard, it is clarified that:

a) Chapter III-A of the Framework Directive, establishing a Community regime governing the security and integrity of networks and services, notwithstanding the concern expressed in Recital 44 of Directive 2009/140/EC regarding critical infrastructure protection (CIP), in an apparent indication of the path that should be followed, does not make a distinction as to the networks and services covered;

b) Similarly, the provisions of Chapter V of Title III of the LCE, which transposed said Chapter III-A of the Framework Directive, and in particular and as relates to the object of this decision, article 54-B and point b) of article 54-E, refer to public communications networks and publicly available electronic communication services, without making any distinction between different networks or services;

c) Consequently, ICP-ANACOM considers that, under national and EU frameworks, the requirement to report security breaches or loss of integrity and their public disclosure, under the terms now being defined, is to be applicable to all public communications networks and all publicly available electronic communication services;

d) Similarly, it should be added that ENISA states that *"in general, considerations about the criticality of an infrastructure served by a telecommunications provider will not be part of the scope of the reporting to*

ENISA (the rationale being that Critical Infrastructure and Critical Information Infrastructure are not subject to the Regulatory Framework for electronic communications)";

e) OFCOM opted for a different approach in its guidelines, based on the proposal of CPNI as referred to in point c) of paragraph 5, i.e., based on apparent criterion regarding CIP;

f) Accordingly, and as set out in points a) and b) of paragraph 4 of Section I of Annex A and in points a) and b) of paragraph 3 of Section I of Annex B, ICP-ANACOM considers that (i) the impact of a breach of security or loss of integrity is to be assessed by reference to all networks and all the services of an undertaking that are affected by it and (ii) the number of subscribers or accesses affected by a breach of security or loss of integrity corresponds to the sum of the number of subscribers or accesses which are so affected and as comprised by the various networks and services

In one example, and considering a breach of security or loss of integrity that affects a company providing (on an aggregate basis or otherwise) the fixed telephone service, Internet access service and signal distribution television service, impacting:

i. 10,000 fixed telephone service subscribers;
ii. 20,000 Internet access subscribers, and;
iii. 20,000 subscribers fixed telephone service, Internet access and TV signal distribution subscribers;

thereby impacting 50,000 subscribers of electronic communications services (although by service it has an impact on 30,000 fixed telephone subscribers, 40,000 Internet access subscribers and 20,000 subscribers of the service signal distribution television service), the impact to be considered for the purposes set out in both Annexes A and B is of 50,000 subscribers.

10) The majority of companies and APRITEL also make reference to the inappropriateness of the obligation under the Draft Decision, of companies to inform the public as to certain security incidents, citing, among other reasons of a legal nature which allegedly require that the public interest analysis be undertaken on a case-by-case basis, issues of any alarm that may be caused among the population, resulting from such disclosure, or even *"sensationalist"* reporting by certain members of the *media*, while also noting that no other NRA has taken a similar approach.

Whereas point b) of Article 54-E of the LCE sets out that the NRA may inform the public, by the most appropriate means, of any breach of security or loss of integrity or require the companies to do so, where it determines that disclosure of the breach is in the public interest:

a) ICP-ANACOM considers that the determination of whether public disclosure of a breach of security or loss of integrity is of public interest, can be performed either *a posteriori*, after verification and taking into account its scale and effects, or *a priori*, by the prior establishment of the characteristics which, for this purpose, a breach of security or loss of integrity shall fulfil;

b) In this respect, and on the one hand, ICP-ANACOM shall, pursuant to the terms of paragraphs 2 and 3 of Point I of Annex B, establish the circumstances in which it considers that the significant impact of a particular breach of security or loss of integrity, in view of its duration and in view of the number of subscribers or accesses affected (or geographical area affected), makes disclosure to the public in the public interest ;

c) On the other hand, and under the terms set out in paragraph 4 of Point I of Annex B, ICP-ANACOM also makes clear that the provisions of this Annex shall be without prejudice, in circumstances not provided for therein and also where there is considered to be public interest, to this Authority being entitled, *a posteriori*, to order the companies to inform the public as to breaches of security or loss of integrity occurring on their networks and services;

d) To this purpose, note is made of some of the security incidents which have been in the news in recent years, even while, as far as we know, having a lesser impact (in terms of number of subscribers / affected accesses) than the lowest threshold set out in the Draft Decision;

e) The companies are certainly equipped with this knowledge, at technical and communication levels, enabling them to inform their subscribers and the general public in a clear, transparent and proper manner, and thereby help avoid any alarm or *"sensationalism"* which might arise if this information were to reach the public by other means (for example, spread rapidly through social networks, not to refer to the examples provided by the companies);

f) As shown by the reading of regulation of FICORA referred to above, ICP-ANACOM's approach is not unique in the sphere of European NRA.

11) The companies in general and also APRITEL, view the deadline of 30 days to

implement the measures in the Draft Decision as tight, seeking a period of at least 6 months following the final decision.

Bearing in mind the responses received regarding the importance given by the companies to the security and integrity of networks and services, and regarding the investments already made, and also the procedures already in place, as on one hand, as well as the decisions of other regulators and the decision of the Commission that the NRA inform the Commission and ENISA as to security incidents recorded between 1 January and 31 December of each year, entering at *"cruising speed"* with the report submitted during 1Q2013 and bearing in mind, on the other hand, other NRA decisions, such as the decision of PTS of 21 February 2012 (entering into force on 1 April 2012), and the decision of FICORA[10] of 23 January 2012 (entered into force on 1 February 2012) and, finally, the time elapsed since the public consultation, ICP-ANACOM believes that the timeframe requested is perhaps extended.

Notwithstanding the above, considering the arguments and trying to reconcile competing interests, ICP-ANACOM will extend the period before entry into force of the measures for a period equal to 6 months, pursuant to paragraph 1 of Section III of Annex A and paragraph 1 of Section III of Annex B.

With regard to Annex A, however, under the terms of paragraph 2 of Section III thereof, the obligation is set out to submit progress reports covering the entire period from 1 January 2013 until the entry into force of this Annex, based on available data and with reference to the circumstances set out in Section I and the requirements for final notification in paragraph 9 of Section II, for respective communication to the European Commission and ENISA, in line with what has been ICP-ANACOM's position in terms of cooperation with these institutions.

12) ICP-ANACOM states that its determination to protect the interests of citizens in this Draft Decision is welcomed by consumer associations.

13) The public entities, at a central (DGC) and regional (GRM) level, which gave their contributions, note in the Draft Decision, consumer protection in the first case, and, in the second case, concerns about the geographic and political-administrative reality of the autonomous regions.

Regarding the comment from DGC as to a lack of reference to the use of different

[10] As regards information to the public (Chapter 3) FICORA set 1 April 2012 as the date of entry into force.

technologies and the respective differences in terms of capacity for action and problem resolution by the companies, it is made clear that, under the provisions of Article 54-B and in paragraph 2 of article 54-C and in point b) of Article 54.-A of the LCE, the resolution of security breaches or loss of integrity are not covered by this decision, which is limited only to the reporting of such incidents and their disclosure to the public.

C – SPECIAL CONSIDERATIONS

A) ANNEX A to the draft decision

- **AT&T, COLT and Verizon Business** draw attention to fact that, despite potentially enjoying national coverage, in general and because of their specificity, customer numbers would not justify the qualification of significant impact, and call on ICP-ANACOM to remove the *"geographical area"* criterion from the decision.
- **CTT** questions the option of measuring geographical area in the context of mobile networks.

  They also report that they will not be covered by the reporting obligation (due to their specificity), refer to the need for ICP-ANACOM to clarify what is meant by *"company"* (I.c) ii) of the draft decision) and to further clarify, respectively in points iii) and iv) of the same section, the terms: *"date which, by its relevance"*, *"geographical impact, especially"* and *"other relevant entities"*.

  CTT also considers that: the number of notifications is high, the deadline for notification is tight, it is difficult to identify the root cause within the stipulated deadline and again that they should not be subject to the reporting obligation since they *"do not make any network information available to ICP-ANACOM"*.

  Finally, the company holds that the implementation period should be extended to 6 months.
- **Cabovisão** refers to the need to consolidate the concept of security incident by reference to continuity of service.

  The company considers that reportable incidents should be those that have a duration of at least 4 hours, recalling the proposals of the ENISA document as regards the expression between the number of subscribers affected and the total number of users of the affected service, and as regards reportable services.

  It cites difficulties in determining geographical area, when assessing the impact of repeated incidents, and in cooperation between companies.

  Cabovisão raises questions regarding the notification of non-delivery of calls to 112 call centres, in the case of one connection failure when there are more available, and where the root cause is responsibility of Portugal Telecom.

  It calls on ICP-ANACOM to define dates and entities referred to in sections I.c) iii) and I.d).

Cabovisão alleges an excess of notifications and calls on the regulator to substantiate the necessity to receive notifications and the use it will make of the reports, not accepting the regulator's proposal as regards as corrective actions to prevent recurrence.

It considers that the notice period should be 2 days, and that a single email address is insufficient.

"For reasons of legal certainty", Cabovisão considers that an exhaustive list of security incident root causes should be established.

Finally it is not clear on the request for the data contained in the notification to be in line with the statistical data submitted on a quarterly basis to ICP-ANACOM, and calls for the implementation deadline to be extended to 6 months.

- **Grupo ONI** calls attention to: the different criteria used in the ENISA document, the consequent confusion between faults and security incidents, and the likely number of notifications concerning the non-availability of the 112 service, given that any incident which affects the voice service for more than 15 minutes is to be notified.

  The Group also refers to the criteria of accumulation of events affecting one or more operators, giving rise to operational problems, to incidents on special dates, requesting their non-inclusion, to incidents that affect networks and services on the islands of the Autonomous Regions, recalling the ENISA criteria of 10% of users and 4 hours of duration, and to the need to list government, regional and other socially relevant bodies, so that companies do not incur non-compliance.

  It considers that the initial notification deadline is too tight, since, it claims, its purpose is statistical, and it asks for a review of the deadline and its alteration to 48 hours; likewise, it considers 3 notifications to be excessive, and calls for the interim notification to be scrapped and the final notification to be submitted one month after the incident ends.

  Finally it requests an extension to the implementation deadline to six months.

- **Optimus** cites the need to clarify the type of incidents to be reported, arguing that reportable incidents should be those affecting the continuity/availability of the service and to clarify the services covered by the notification, calling, in particular, for the exclusion of television services (*"this service was not considered relevant by ENISA"*).

  As regards the thresholds, it seeks clarification as to their being cumulative, considers notification of incidents of less than four hours to be unwarranted, and cites difficulties in determining the affected area.

As regards 112 calls, it considers that only incidents which prevent the delivery of calls to the PSAP originating on fixed networks and having a duration of less than one hour should be notified.

For repeated incidents and incidents impacting the networks or services of various companies, it seeks their exclusion, citing difficulties in their determination and also issues of confidentiality in the second hypothesis.

It claims equal difficulties for incidents occurring on special dates, and calls for a re-assessment as to the reporting of incidents in the autonomous regions;

It questions the SIRESP example shown because *"this is a system that should be independent of commercial communications operators"*;

As regards government or regional customers, in addition to claimed difficulties in implementation, it cites legal constraints with respect to the differential treatment of the different users.

It presents the following proposal on reportable incidents:

		Notification to ICP-ANACOM			Disclosure to the public	
Initial notification deadline►		4 working hours			4 working days*	
Services▼		**duration ≧**	**PASP ≥**		**duration ≧**	**PASP ≥**
112 (Fixed)		1	1		4	1
Services▼		**duration ≥**	**customers ≥**		**duration ≥**	**customers ≥**
Fixed Voice		1	450,000			
		2	300,000			
		4	150,000			
		6	60,000			
		8	30,000		8	150,000
Mobile Voice; SMS		1	2,250,000			
		2	1,500,500			
		4	750,000			
		6	300,000			
		8	150,000		8	750.000
Internet (Mobile; Fixed)		1	2,700,000			
		2	1,800,000			
		4	900,000			
		6	360,000			
		8	180,000		8	900,000

Legend:
Duration - likely minimum duration of the incident in hours (according to the ENISA scale)
Customers - minimum number of subscribers/access affected
PASP - Pontos de Atendimento de Segurança Pública (Public Safety Answering Points - 112/115 call centres).
* Disclosure to the public undertaken only after ANACOM approval/decision
- Incidents covered by this threshold should NOT be reported
- Incidents covered by this threshold should be reported

Interpretation of the table:
1 - Identify type of service
2 - Locate, moving line by line, the thresholds applicable to the type of service
3 - If at least one line applies according to both criteria (duration + customers or PASP), select this line
4 - If the line is marked in red, then the incident is reportable

It suggests notification by additional means as well as e-mail and use of *"mechanisms of authentication, integrity and non-repudiation, such as digital certification"*.

It stresses the claimed operational difficulty, in terms of cooperation between companies, of aspects relating to detection, assessment and reporting, and cites issues with sharing confidential information, proposing a reassessment of this obligation.

As regards the identification of cause, the company cites difficulties in the case of external suppliers (such as energy suppliers).

It requests clarification regarding the draft decision's reference to statistical data submitted to ICP-ANACOM on a quarterly basis.

As regards the initial notification, it disagrees with a 2 hour deadline and proposes 4 hours; it suggests that *"final notification"* be made an *"Incident Report"* with a longer period for submission, and raises several doubts as regards the interim notification, namely that it should be optional.

- **Grupo PT** calls for a definition of *"incident"*, proposing *"an event that has an impact on one or more network elements with the same root cause"*.

  It calls for it to be established that *"reporting requirements should only cover incidents with a significant impact on the operation of networks or provision of services or which affect the continuity/availability of networks and services"*, and cites potential difficulties in implementing the geographical criteria.

  It argues that thresholds should be applied by service, according to criticality, referring to those identified by ENISA (Fixed Voice, Mobile Voice, SMS, Internet, e-mail), reproducing the table of thresholds contained in the document published by ENISA:

Duration / Subscribers/Accesses	**1h-2h**	**2h-4h**	**4h-6h**	**6h-8h**	**>8h**
1% - 2% of subscribers/accesses					X
2% - 5% of subscribers/accesses				X	X
5% - 10% of subscribers/accesses			X	X	X
10% - 15% of subscribers/accesses		X	X	X	X
>15% of subscribers/accesses	X	X	X	X	X

It mentions the possibility of border situations in relation to violations of personal data which should be *"excluded from the reporting obligation applicable to services that are provided over the network of a given operator"*.

As regards 112 incidents, the company argues that notification should be made based only on the MAI's involvement in the fault[11] and, in relation to calls originating on mobiles, that these should be excluded because the call could be made through another operator.

With regard to point I.c), Grupo PT states, respectively: (i) that it has no opposition if the regulator follows their proposals/table, otherwise it is inappropriate, (ii) it is infeasible and proposes it be removed, (iii) the relevant dates should be previously defined and announced by ICP-ANACOM, and for incidents lasting more than one hour; (iv) should be for events lasting more than one hour.

On section I.d), Grupo PT states that, the contracts with the entities mentioned contain confidentiality clauses, whereby ICP-ANACOM should collect the required information from these entities directly.

Grupo PT considers the notification process to be excessively bureaucratic, whereby, in its opinion, it is essential to define who is responsible for coordinating cooperation between companies, and that notification is made after resolution of the incident;

It holds that submission by e-mail does not guarantee necessary security, so that a process should be implemented which does;

Grupo PT does not perceive the meaning and scope of the reference to *"statistical data provided to ICP-ANACOM on a quarterly basis"*, given the specific purposes of the data provided by the companies.

It suggests creating a *"template"* for notifications, for harmonization of reports by companies with this obligation, including MVNOs, and reaffirms the need for procedures in this matter to be brought into line with the Privacy Directive.

Finally the Group proposes that the initial notification deadline should be extended to 8 working hours, the interim notification deadline should be set at 8 working hours from cessation of the incident (where cessation is not covered by the initial notification), and that the information to be provided in the final notification should be optional; it calls on ICP-ANACOM to consider an implementation period of at least 6 months.

[11] Ministry of Internal Affairs.

- **Vodafone "S.I.C. [Start of Confidential information]**
  E.I.C. [End of Confidential information]
- **APRITEL** considers, on an introductory basis, that only incidents which cause service disruption should be reported, and not incidents that temporarily affect quality of service, that the criteria should be in line with *"the guidelines issued by ENISA"*, and that the procedures are too demanding, raising the possibility of a high volume of notifications which *"may even clog up the regulatory system"*.
  It notes that the draft decision does not set out which services are subject to reporting, and *"it holds that ICP-ANACOM must clarify its position concerning the operations of preventive and/or corrective maintenance or planned network improvements"*.
  It considers that the thresholds are set too low, and, as an example, claims *"some incidents of such short duration (15 minutes) may not be detectable"*.
  It holds that for impact assessment only *"subscribers/accesses" should be considered* because their combination with *"geographical area"* makes for an overly onerous and complex process, and it refers to the impossibility of determining customers affected on the mobile service.
  As regards the impact on access to the single European emergency number, APRITEL supports, in the case of fixed services, following ENISA with respect to the combination of percentage of affected subscribers/accesses and duration of the incident, whereas mobile should not be considered, as when the network is unavailable calls can still be placed through another mobile network.
  It considers reporting repeated incidents (I.c) (i)), and with cumulative impact on several companies (I.c) (ii)) to be unworkable; as regards special dates, it considers that the companies should be informed beforehand (I.c) (iii)), and as regards government and regional entities (I.d)), it will be necessary to define a prior list, that the example of SIRESP is questionable, since *"the failure of operator services should not impact SIRESP"*, and that it is important to safeguard legal issues since *"operators are subject to an obligation of non-discrimination"*.
  The Association takes the view that the number of notifications is excessive, having no parallel in the positions taken by ENISA or other regulators, such as OFCOM, and questions *"the necessity or usefulness of ICP-ANACOM receiving such a number of notifications, since it ultimately may not be able to analyze (or even receive) so much information"*.

APRITEL considers that notification by e-mail is insufficient, and that the content should be safeguarded; cooperation in reporting a single security incident is not feasible for companies; and that when the cause is a failure by an external service provider (supplier of energy or other operator), it is not always possible to obtain information in the short/medium term on the causes and the estimated time of resolution.

It suggests that the initial notification be made within 2 working days and final notification be known as *"Incident Report"*.

It calls for the adoption of a common *"template"* and notes that, if the range of eligible services is not limited and the criteria of duration and the number of subscribers or affected area are not made more flexible, its members will have to channel efforts towards the formulation of reports, shifting focus away from the fundamental issue (to ensure maintenance of the network and services).

Finally it describes the period of 30 days from entry into force as unworkable and unacceptable, and proposes a minimum period of six months.

- **GRM**, in view of the ultra peripheral condition of Madeira, considers that *"a reduction in the thresholds underlying the criteria of number of subscribers/access and/or geographical area set out in the table may be warranted"*.

POSITION OF ICP-ANACOM

The reasoning that supports the final version of Annex A is set out below, with the following amendments highlighted:

- Adjustments in the thresholds set out in the table in point a) of paragraph 3 of Section I, both as regards duration and as regards the number of subscribers or accesses affected (or geographic area affected);
- Elimination of the reporting obligation as applicable to a set of companies affected by the same breach of security or loss of integrity, with the exception of the condition now set forth in point g) of paragraph 3 of Section I;
- The time limit of the initial notification calculated from the moment the company ascertains the circumstance which, in the specific case, determined the reporting obligation laid down in paragraph 4 of Section II; as such there can be no doubt as to the existence of significant impact at the time of notification;
- Clarification of the circumstances that constitute significant impact and determine the reporting obligation laid down in paragraphs 2 et seq. of Section I, noting the

restriction of the criterion as regards *"affected geographic area"* to cases where the criterion on the number of *affected subscribers or accesses* is not applicable or, in the specific case, demonstrated as impossible to determine or estimate, in accordance with the provisions of point e) of paragraph 4 of Section I;

- Extension of the period of entry into force to six months, as set out in paragraph 1 of Section III.;
- Provision, on a transitional basis and pursuant to paragraph 2 of Section III, for an obligation to submit reports with respect to the period between 1 January 2013 and the entry into force of this Annex A.

1. The new regulatory framework governing security and integrity of networks and services, as results from the provisions of Chapter III-A of the Framework Directive and, in Portugal, Chapter V of Title III of the LCE, and in particular as governing the subject matter of the draft decision, essentially sets out characteristics of transparency, both with regard to the reporting of security breaches or losses of integrity to the respective NRAs and annual reporting by NRAs to the European Commission and ENISA, either in the context of their disclosure to the public or, where so determined, by the companies themselves (often just before such incidents are reported by the news media, sometimes in an unclear and/or inaccurate manner).
2. It is an important point to make that a very high number of notifications is neither a likely nor desirable outcome; nor is a very low number of notifications, which loses sight of the objective stemming from the recent content of the regulatory framework. As such, the quantity of notifications should be sufficient to enable conclusions to be drawn with some soundness and significance, without prejudice to the possibility of revising the dimensions now used in criteria to determine significant impact, as requiring notification, with a view to their improvement, as is indeed cited in the draft decision.
3. It is to be noted that, in our view, there is no confusion between faults and security incidents because a fault is included in security incidents (e.g., if hardware, the root cause will be included in the category *"hardware failure"*).

As regards our position on *"Preventive and/or corrective maintenance or*

planned network improvements"[12], there can only be one: where these result in significant impact, these must be reported.

4. Regarding Grupo PT's proposal for a definition of *"incident"*, this is not accepted, for reasons already referenced, such as, for example, that ITU Recommendation E.409[13], defines *"event"*, *"incident"*, and *"security incident"*, and was not considered in the Directive, i.e., this is not deemed to have restricted, by definition, the scope of reportable security incidents.
5. As regards identification of security breaches or loss of integrity which are reportable pursuant to paragraph 2 of Section I of Annex A, it is considered that all breaches of security or loss of integrity are reportable as cause a serious disturbance to the functioning of networks and services, with a significant impact on the continuity of this functioning, according to the circumstances and the rules laid down in paragraphs 3 et seq. of the same Section I.
6. For the purposes of assessing the impact of a determined breach of security or loss of integrity and the subsequent evaluation of its nature as significant or not significant, under the terms defined in the points of paragraph 4 of Section I of Annex A, the following rules are to be observed:
    a) The impact of a breach of security or loss of integrity is to be assessed by reference to all networks and all the services of a undertaking that are affected by it;
    b) The total number of subscribers or accesses affected by a breach of security or loss of integrity corresponds to the sum of the number of subscribers or accesses affected thereby on the various networks and services[14];
    c) The number of subscribers to a service that is supported over another service will only be recorded when the support service has not been affected[15];
    d) The number of subscribers or accesses affected corresponds to the

[12] In principle, it does make sense that these measures would have a significant impact; on the other hand, we are already aware of several such actions, in which it was supposed there would be no significant impact, but which resulted in significant security incidents with particular impact, and for example, alleged human error.
[13] International Telecommunication Union.
[14] *See* for example in point f) of section 9 of our positions as regards *"general considerations"*.
[15] For example, in the case of SMS, it only counts if the supporting telephone service is not be affected.

number of subscribers or accesses covered by the breach of security or loss of integrity (or, in other words, the number of subscribers or accesses for whom the network is potentially available under normal conditions of functioning), or where it is not possible to determine this number, to an estimate based on statistical data held by the company;

e) The criterion related to affected geographical area is only to be applied in the event that the criterion on the number of affected subscribers or accesses is inapplicable or, in the specific case and on a reasoned basis, impossible to determine or estimate, as would be the case, perhaps, of broadcasting services;

f) The circumstances described in paragraph 3 of Section 1 of Annex A must be assessed in relation to a company considered individually, or in the case of the circumstances referred to in point a), and in the part that refers to this point, in c), both of the same paragraph 3, also in relation to a set of companies which are covered by the conditions laid down in paragraph 2 of article 3 of Law no. 19/2012 of 8 May. This option, taking into account the provisions of Article 54-B of the LCE, is based on the need to obtain information in relation to the overall size of a particular incident which, in its impact on the companies comprising a set of companies in these conditions, attained significant impact; in this respect, ICP-ANACOM deems it proportional and appropriate that, for this purpose, it requires such companies, in accordance with paragraph 13 of Section II of Annex A, to coordinate in detection, evaluation and joint notification.

7. From what we know, in particular from the ENISA and OFCOM documents and FICORA and PTS regulations, we concede that this position in part and apparently has no parallel from another European regulator, but we are convinced that this is the correct interpretation of the provisions of the law, at risk of security incidents with a significant impact on a large number of users not being reported just because they use different services or a single service supported over different networks, while nevertheless having a common cause - the same security incident.
8. As regards point a) of Section I of Annex A of the draft decision, now point a) of paragraph 3 of Section I of Annex A, the following is clarified:

a) The criteria *"duration"*, on the one hand, and *"number of subscribers or accesses affected (or under the terms of point e) of paragraph 4 Section I, geographic area affected)"* are cumulative, as is apparent from the conjunction *"and"* as already set out in the draft decision and maintained in the decision's final version;

b) The number of thresholds is maintained, but adjusted, with the major difference in the subcriterion *"geographic area affected"*, bearing in mind that, pursuant to point e) of paragraph 4 of Section I of Annex A and in view of the comments received in this regard, the application of this criterion[16] is now residual, applying only in cases where the criterion concerning the number of affected subscribers or accesses is inapplicable or, in the specific case and on a reasoned basis, impossible to determine or estimate;

c) Grupo PT's proposal for this section stems from the proposal of ENISA which, having a different goal and emphasizing a rationale that is distinct from that resulting from ICP-ANACOM's interpretation of the provisions of the LCE, and is not accepted;

d) As regards the proposal put by Optimus, this would enable the possibility of this company's network being inoperative for a period of up to four (4) hours with no obligation to notify; this makes no sense.

9. As regards point b) of Section I of Annex A of the draft decision, now point b) of paragraph 3 of Section I of Annex A, the following position is taken:

a) Further to the previous point, it is necessary to consider first and foremost, ICP-ANACOM's responsibilities as regards the single European emergency number 112, under the provisions of article 5[17] of Decree-Law no. 73/97 of 3 April, as well as paragraph 2 of article 49 of the LCE as regards the duty of undertakings providing publicly available telephone services to take all necessary measures to ensure uninterrupted access to emergency services;

[16] That however must continue to be estimated and referenced, as a minimum, in the final notification.

[17] *"The Ministry of Provision, Planning and Territorial Administration shall, through Instituto das Comunicações de Portugal (Portuguese Communications Institute), be responsible for necessary coordination with public telecommunications operators and for adjustments to the basic telecommunications and cellular telephone networks so that all calls made to telephone number 112 are answered by an emergency telephone exchange."*

b) What is at stake here is the connectivity of companies, directly or indirectly (through another interconnected company), to the emergency services;

c) It does not make sense that a company offering a mobile network should be exempt from reporting as sought by APRITEL in particular, with the argument that calls to 112 may be made through another network if the native network is unavailable, not least because: emergency calls may also be made through the national emergency number 115, or the network may not be affected not at radio level but at core level and in this case we do not have the information that what APRITEL refers to is guaranteed; on the other hand it may also happen that other mobile networks cannot deliver emergency calls and then in that case, no company would report the situation, and furthermore, as referenced, since it is important to be aware of what is occurring on electronic communications networks and services in terms of security and integrity;

d) It should be kept in mind that on this issue the ENISA document says *"This can be a stand-alone parameter meaning that if an incident impacts on emergency calls, the reporting scheme is triggered regardless of the duration or users affected"*, which we follow in this case, while granting that, solely for the purpose of reporting and at this time, only security incidents lasting at least 15 minutes are considered;

e) In the case of one interconnection failing when there are more available, as raised by Cabovisão, provided that the company continues to deliver calls directed to PASP at another point[18], it will not be obliged to notify; as to the possibility that the security incident might have *"root cause"* at Portugal Telecom but also impact Cabovisão, the view is taken, at present, that it is the party that fails to provide their subscribers with uninterrupted access to emergency services which should always provide notification, notwithstanding that the other company may also provide notification and notwithstanding that the responsibilities of the companies in terms of security and integrity of

[18] Pontos de Atendimento de Segurança Pública (Public Safety Answering Points - 112/115 call centres).

networks and services go beyond notification;

f) In conclusion, if a company fails to deliver 112 calls, whether directly to the PASP or indirectly through another company with which it has interconnection,[19], it is bound to provide notification.

10. As regards point c) of Section I of Annex A of the draft decision, now points c), d), e) and g) of paragraph 3 of Section I of Annex A, the following position is taken:

a) As regards item i) of point c) of Section I of Annex A of the draft decision, now point c) of paragraph 3 of Section I of Annex A, it is important to be aware of, examine and possibly take measures on a specific security incident which, reoccurring over a period of four weeks[20], has a significant accumulated impact falling within the circumstances listed in point a) or b) of the same paragraph 3 of Section I; as such, it is necessary to consider security incidents that have the same origin, especially in terms of root cause and affected network element(s) or system(s);

b) With regard to item ii) of point c) of Section I of Annex A of the draft decision, this final decision omits the obligation to report security incidents having a significantly impact on various companies, with the exception of the situation envisaged in point g) of paragraph 3 of Section I of Annex A;

c) As regards item iii) of point c) of Section I of Annex A of the draft decision, now point d) of paragraph 3 of Section I of Annex A, it is also important to be aware of, examine and possibly take action on a particular incident security which has a duration of less than one hour and affects 1,000 or more subscribers or accesses, or which, under point e) of paragraph 4 of the same Section, affects a geographical area equal to or exceeding 100 km^2, when this security incident occurs on dates on which the normal and continuous operation of networks and services is particularly important, in particular the dates already identified under the terms of paragraph 5 of the same Section I and those which, according to the provisions in this same paragraph, may

[19] Includes calls made by dialling 115.
[20] It is considered preferable to establish a specific and unvarying time limit of 4 weeks, as opposed to a variable time limit of one month.

be identified by ICP-ANACOM;

d) With regard to item iv) of point c) of Section I of Annex A of the draft decision, now point e) of paragraph 3 of Section I of Annex A, due to the specificity of the Autonomous Regions of the Azores and of Madeira (composed of islands) and taking into account the comments submitted by GRM, ICP-ANACOM considers it important to have notification of security incidents which occur in these regions having a duration equal to or greater than 30 minutes and which affect the functioning of all networks and services offered by the same company in the entire territory of an island (i.e., when a company is prevented from continuing to provide users with their entire offer on a given island), regardless of the number of subscribers or accesses affected or of the geographic area affected.

11. We cannot omit to point out the provisions of Recital 44 of Directive 2009/140/EC: *"Reliable and secure communication of information over electronic communications networks is increasingly central to the whole economy and society in general. System complexity, technical failure or human mistake, accidents or attacks may all have consequences for the functioning and availability of the physical infrastructures that deliver important services to EU citizens, including e-Government services"*.

This is the rationale underlying point d) of Section I of Annex A of the draft decision, and is, in our view, in keeping with the spirit of Community and national frameworks, when provision is made respectively in paragraph 1 of article 13-A of the Framework Directive and paragraph 1 of article 54-A of the LCE, that measures are to be taken to prevent or minimize the impact of security incidents on users and *"interconnected networks"*. In particular, the term *"interconnected networks"* is not restricted, in this case and as held by ICP-ANACOM, only to the *interconnection* of public communications networks, but includes networks/*"physical infrastructure through which important services are provided to EU citizens, including e-government services"*, which services are supported over public communications networks or publicly available electronic communication services and which, to serve citizens, require reliable and secure communications.

As such, and given the duties and powers conferred upon ICP-ANACOM as

regards security and emergency issues, ICP-ANACOM considers that any breach of security or loss of integrity should be notified, where detected by these companies or where reported to companies by customers, as have impact on the functioning of networks and services through which services are provided which are relevant to society and to citizens by the public or private entities, on a national or regional basis, referenced in paragraph 6 of the same Section I, provided the incident has a duration equal to or greater than 30 minutes.

Also on this point and with respect to obligations of confidentiality to which Grupo PT claims to be subject and which *"prevent sharing of information, whatever it may be"*, it is clarified that:

a) Under the provisions of paragraph 1 of article 108 of the LCE, bodies subject to obligations under the present law shall provide to ICP-ANACOM all the information related to their activity, so that ICP-ANACOM is able to exercise all powers provided for in the law;
b) The information to be transmitted is covered by the obligation to notify ICP-ANACOM as arising from Article 54-B of the LCE, given the need to exercise powers which are conferred upon ICP-ANACOM in this respect, and therefore cannot be excluded from the outset on the basis of an obligation of confidentiality that is exclusively contractual in origin;
c) Companies subject to the reporting obligation shall identify, in a reasoned manner, such information as they deem confidential and attach, where appropriate, a non-confidential version of the documents comprising such information, pursuant to paragraph 3 of article 108 of the LCE and in accordance with ICP-ANACOM decision of 17 November 2004;. and
d) ICP-ANACOM is subject to confidentiality requirements, pursuant to the Código do Procedimento Administrativo (Administrative Proceeding Code), to Law no. 46/2007 of 24 August, the LCE, its Statutes (as approved by Decree-Law no. 309/2001 of 7 December), and pursuant to other applicable legislation.

However, because it is conceded that it is relevant to examine the various relationships with different stakeholders on this issue and on terms that are set out in paragraph 6 of Section I of Annex A, identification of relevant entities for

the purposes of point f) of paragraph 3 of Section I will be undertaken subsequently by ICP-ANACOM and duly notified to the companies within a minimum of five working days. The only exception which it is deemed important to define at this time relates to SIRESP - Sistema Integrado de Redes de Emergência e Segurança de Portugal (Integrated Security and Emergency Network System) which, contrary to what is stated by Optimus and APRITEL, is not independent of the services of the companies, as ICP-ANACOM had opportunity to demonstrate during the PROCIV V exercise, organized by ANPC[21] on 17 November 2011.

Finally, as regards the position of Optimus as to *"Safeguarding legal issues regarding the differential treatment of the distinct users, given that (...) operators are subject to an obligation of non-discrimination with regard to end-customers"*, it is clarified that the circumstance referred to in point f) of paragraph 3 of Section I of Annex A is justified by the importance of the services provided to society and to citizens by the end-users in question, which importance, in observance of the principle of equality in its material aspect, requires, in this respect, differential treatment in relation to other end-users.

12. Regarding the number of notifications, the following position is taken:
    a) The following notifications will take place: an initial notification, a notification of the cessation of the security breach or loss of integrity with significant impact, given the importance of being informed as to the cessation of significant impact, and a final notification;
    b) In the circumstances set out in points c) and g) of paragraph 3 of Section I of Annex A, the companies will submit, respectively, only a final notification or may submit a single series of notifications, as now set out in paragraphs 2 and 3 of Section II of Annex A, and in light of the specific nature of the situations to which they refer.
    c) At this time, the proposal for a *template* similar to that proposed in ENISA's document (while not for the same purpose) or in the OFCOM document is not accepted, since such a step would, at present, be premature; this was not an option taken by FICORA or PTS;
13. Pursuant to paragraph 12 of Section II of Annex A, the initial notifications and

[21] Autoridade Nacional de Proteção Civil (National Civil Protection Authority).

notifications of cessation of a breach of security or loss of integrity with significant impact are to be made immediately by email or by telephone, in both cases within the stipulated deadline; the telephone number will be used to notify the relevant information, in the event that there are problems with the email or to confirm receipt of information by email. The final notification should be submitted in person or by registered mail;

14. At a time when information sharing, particularly with regard to security, is considered essential to ensure a proper response to the challenges faced in this context by companies and stakeholders (e.g. CSIRT networks[22], as underlined by APRITEL), we maintain the provisions of the draft decision as regard a duty of cooperation between the companies whose networks or services are impacted in their functioning by the same breach of security or loss of integrity, to provide for proper detection and assessment of the impact of this breach of security or loss of integrity and, in the case covered by point g) of paragraph 3 of Section I of Annex A, to provide for respective notification, as stipulated in paragraph 13 of Section II of Annex A.
15. With respect to point d) of paragraph 5 and point a) of paragraph. 7, in point e) of paragraph 9 and paragraph 10 of Section II, it is recommended that the causes root are reported to ICP-ANACOM in accordance with the lists set out in the document *"Technical Guidelines on Incident Reporting"*, published by ENISA, where applicable.
16. The obligation of submitting, whenever possible, the information which is to be notified to ICP-ANACOM to the definitions set out in the context of the obligations to report periodic information to ICP-ANACOM, pursuant to paragraph 11 of Section II, is justified given the need to try to follow what has already been harmonized in this area, in order that ICP-ANACOM is able to conduct proper analysis, in terms of number of subscribers or accesses.
17. The priority given at the end of paragraph 4 of Section II to the mitigation and resolution of any breach of security or loss of integrity in relation to its initial notification is limited to the obligation to notify ICP-ANACOM in a timely manner, as is expressly safeguarded in the same context.
18. In accordance with the provisions of article 54-B of the LCE, ICP-ANACOM considers it should clarify that the obligation to report breaches of security or

[22] *Computer Security Information Response Team*.

losses of integrity with significant impact necessarily entails an obligation to conduct preliminary assessment of the impact of the incidents occurring, an obligation whose fulfilment companies may not, in any event, avoid or transfer to ICP-ANACOM.

In this regard, in accordance with the provisions of the new paragraph 14 of Section II of Annex A and in order to fully comply with the provisions of this Annex A, it is determined that the companies have responsibility for implementing all the means and procedures necessary to ensure detection, impact assessment and reporting of security breaches or losses of integrity covered by the conditions laid down in Section I of Annex A.

19. Concerning the deadlines for notification:
    a) The deadlines governing notification to ICP-ANACOM should facilitate analysis of significant impact by the companies with reference to the actual duration and not likely duration as set out in the draft decision;
    b) Accordingly, and pursuant to paragraph 4 of Section II, initial notification is to be sent as soon as the company is able conclude that there is or will be significant impact, up to one hour after ascertaining the circumstances set out in Section I that, in the specific case, determined the reporting obligation, that is, up to one hour after the end of the period which, in the specific case, determined the reporting requirement, so that the provision made in the draft decision for the possibility that a security incident cannot attain significant impact no longer makes sense.
    c) For the purposes of paragraph 3 of Section I, the duration of a determined breach of security or loss of integrity and the notification deadlines are continuous, whereby the proposal that such deadlines be calculated in working hours cannot be accepted;
    d) The interim notification is therefore dispensed with and instead takes the form of a notification of cessation of a security incident with significant impact, to be submitted to ICP-ANACOM as soon as possible and within a maximum period of two hours following cessation of significant impact, unless this cessation has already been reported in the initial notification, as provided for in paragraph 6 of Section II;
    e) Pursuant to paragraph 8 of Section II, final notification is to be sent to

ICP-ANACOM within a period of twenty working days from the moment the breach of security or loss of integrity ceases to have significant impact, which moment might not coincide with full resolution of the security incident. As such, a substantially longer period is granted for performance of this final notification, so that the information submitted can be made as complete and detailed as possible, seeking to avoid further iteration between ICP-ANACOM and the companies.

20. As regards the content of the notifications, our position should be noted as regards the following points:
    a) Although, at this time, for the purpose of significant impact, the *"affected geographic area" criteria are considered* only in a supplementary manner, in accordance with point e) of paragraph 4 of Section I, it remains important to estimate the geographic area affected; as such, indication is required in the final notification, in accordance with the provisions of item v) of point d) of paragraph 9 of Section II, and where estimation is possible, in the initial notification in accordance with the provisions of item iv) of point e) of paragraph 5 of the same Section;
    b) The initial notification must include the information referred to in points a) to d) of paragraph 5 of Section II, as well as the best estimate of its impact in terms of affected networks and services, in terms of access to emergency services, in terms of affected subscribers or accesses and affected geographic area, as stipulated in point e) of the same paragraph;
    c) Pursuant to and under the terms of articles 108 and 109 and in view of paragraph 2 of article 54-G and article 112 of the LCE, ICP-ANACOM may, at any time, request information relating to the security incident, including through contacts provided by the company in the initial notification;
    d) The final notification shall contain, in detail, the information required under paragraph 9 of Section II of Annex A, including, with regard to:
        1) The root causes, in accordance with point e) of said paragraph 9, for which purpose, where applicable, it is recommended that companies use the list provided in the

document "*Technical Guidelines on Incident Reporting*", published by ENISA;

2) All networks and all services affected and, within each network or service, the number of subscribers or accesses affected, and the number of affected subscribers or accesses represented as a percentage of total subscribers or accesses, under the terms of items iii) and iv) of point d) of the same paragraph 9;

3) The measures referred to in points f) and h) of said paragraph 9 which, contrary the comments submitted by Cabovisão, are crucial in order to ensure the security and integrity of networks and services.

21. As regards entry into force, beyond what has already been cited and in view of the adjustments made to the text of the final decision over the text of the draft decision, given the obligations that remain both for the companies and for ICP-ANACOM, the companies are required to report security breaches or losses of integrity to ICP-ANACOM where ascertained by that date in the manner specified in the transitional provision set out in paragraph 2 of Section III of Annex A.
22. For reasons of clarity and precision, Annex A is reformulated, with a particular focus on the rearrangement of the provisions contained therein.

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

FINAL VERSION OF THE ANNEX A

Circumstances, format and procedures applicable to the requirements of reporting security breaches or loss of integrity with significant impact on the functioning of public communications networks and publicly available electronic communication services

I. Circumstances

1. Pursuant to article 54-B of Law no. 5/2004 of 10 February, as amended and republished by Law no. 51/2011 of 13 September (hereinafter the "Electronic Communications Law"), undertakings providing public communications networks or publicly available electronic communications services (hereinafter, the "undertakings") are required to notify ICP - Autoridade Nacional de Comunicações (ICP-ANACOM) as to any breach of security or loss of integrity with a significant impact on the functioning of networks or services which they provide.

2. Undertakings are required to provide notification of all breaches of security or losses of integrity as cause a serious disturbance to the functioning of networks and services, with a significant impact on the continuity of this functioning, according to the circumstances and the rules laid down in the following paragraphs.

3. For the purposes of the preceding paragraphs, undertakings are required to notify ICP-ANACOM as to:

a) Any breach of security or loss of integrity whose impact is encompassed by the following criteria:

Duration and	**Number of affected subscribers or accesses** **(or, pursuant to point e) of paragraph 4 of Section I, geographic area affected)**
≥ 30 minutes	number of affected subscribers or accesses ≥ 500,000 (Or, pursuant to point e) of paragraph 4 of Section I, geographic area affected ≥3.000 km^2)
≥ 1 hour	500,000 > number of affected subscribers or accesses ≥ 100,000 (Or, pursuant to point e) of paragraph 4 of Section I, 3,000 km^2 > geographic area affected ≥ 2.000 km^2)

≥ 2 hours	100,000 > number of affected subscribers or accesses ≥ 30,000 (Or, pursuant to point e) of paragraph 4 of Section I, 2,000 km^2 > geographic area affected ≥ 1,500 km2)
≥ 4 hours	30.000 > number of affected subscribers or accesses ≥ 10.000 (Or, pursuant to point e) of paragraph 4 of Section I, 1,500 km^2 > geographic area affected ≥ 1,000 km^2)
≥ 6 hours	10.000 > number of affected subscribers or accesses ≥ 5.000 (Or, pursuant to point e) of paragraph 4 of Section I, 1,000 km^2 > geographic area affected ≥ 500 km^2)
≥ 8 hours	5.000 > number of affected subscribers or accesses ≥ 1.000 (Or, pursuant to point e) of paragraph 4 of Section I, 500 km^2 > geographic area affected ≥ 100 km^2)

b) Any breach of security or loss of integrity affecting delivery to Postos de Atendimento de Segurança Pública (Emergency Service Call Centres - 112 emergency calls), directly or indirectly, of calls to the single European emergency number 112, as well as calls to 115 (national emergency number), for a period equal to or exceeding 15 minutes;

c) Any recurrent breach of security or loss of integrity, where the cumulative impact of their occurrences over a four week period is covered by one of the conditions set out in the preceding paragraphs;

d) Any breach of security or loss of integrity which occurs on a date on which the normal and continuous functioning of networks and services is particularly relevant, under the terms of paragraph 5 of this Section I, where the occurrence:

   i) has a duration equal to or exceeding one hour; and

   ii) affects one thousand or more subscribers or accesses, or, under the terms of point e) of paragraph 4 of this section I, ii) affects a geographical area equal to or exceeding 100 km^2;

e) Any breach of security or loss of integrity which impacts the functioning of all networks and services offered by a company in the entire territory of an island of the Autonomous Region of the Azores or of Madeira, where the duration thereof is equal to or exceeds 30 minutes, regardless of the number of subscribers, number of accesses and geographic area affected;

f) Any breach of security or loss of integrity, detected by the undertakings or reported by customers, which impacts the functioning of networks and services through which services with relevance to society and to citizens are provided, by public or private undertakings and at national or regional level, as set out in paragraph 6 of this Section I, where the occurrence is of a duration equal to or exceeding 30 minutes; and

g) Any breach of security or loss of integrity whose cumulative impact on a group of companies which are covered by the conditions laid down in paragraph 2 of article 3 of Law no. 19/2012 of 8 May is covered by the conditions laid down in point a), and, insofar as it refers to the present point, in point c), both of the present paragraph 3.

4. For purposes of the preceding paragraph:

a) The impact of a breach of security or loss of integrity is to be assessed by reference to all the networks and all the services of a company that are affected thereby;

b) The number of subscribers or accesses affected by a breach of security or loss of integrity corresponds to the sum of the number of subscribers or accesses which are so affected and as comprised by the various networks and services;

c) The number of subscribers to a service that is supported by another service will only be taken into account when the support is not affected;

d) The number of subscribers or accesses affected corresponds to the number of subscribers or accesses covered by the breach of security or loss of integrity, or where it is not possible to determine this number, to an estimate based on statistical data held by the undertaking; and

e) The criterion related to the affected geographical area is only to be applied in the event that the criterion on the number of affected subscribers or accesses is inapplicable or, in the specific case and on a reasoned basis, impossible to determine or estimate.

5. For the purposes of point d) of paragraph 3 of the present Section I, notwithstanding the identification of other dates by ANACOM, as duly notified to the undertakings a minimum of five working days in advance, the following dates are deemed relevant:

a) days on which national elections are held (parliamentary, presidential, European or local);

b) days on which national referendums are held;

c) days of national exercises involving electronic communications networks or services, pursuant to point c) of article 54-D of the Electronic Communications Law; and

d) days on which regional elections are held, where security breaches or losses of integrity occur in the region in question.

6. For the purposes of point f) of paragraph 3 of the present Section I, and notwithstanding the possible identification of other bodies by ANACOM, as duly notified to the undertakings a minimum of five working days in advance, SIRESP - Sistema Integrado de Redes de Emergência e Segurança de Portugal (Integrated Security and Emergency Network System) is deemed a relevant body.

II. Format and Procedures

1. For every breach of security or loss of integrity that is subject to notification under the provisions of Section I, undertakings are required to submit the following to ICP-ANACOM:

a) an initial notification, pursuant to paragraphs 4 and 5 of the present Section II;

b) a final notification, pursuant to paragraphs 8 and 9 of the present Section II; and

c) whenever required, in accordance with the provisions of paragraph 6 of the present Section II, notice of the cessation of the breach of security or loss of integrity with significant impact, in accordance with paragraphs 6 and 7 of the present Section II.

2. In the circumstance detailed in point c) of paragraph 3 of Section I, undertakings are only required to submit a final notification to ICP-ANACOM, pursuant to paragraphs 8 and 9 of this Section II, *mutatis mutandis*.

3. In the circumstance referred to in point g) of paragraph 3 of Section I, a single series of notifications may be submitted to ICP-ANACOM, pursuant to paragraph 1 of this Section II, provided that said notifications:

a) cover the entire impact of the security breach or loss of integrity; and

b) are submitted on behalf of all the undertakings.

4. The initial notification is to be sent at the earliest opportunity and when the company is able to conclude that there is or will be significant impact, up to one hour subsequent to ascertaining the circumstance detailed in Section I as, in each specific case, determines the obligation of notification, whereas the undertaking, notwithstanding compliance with this deadline, is required to give priority to the mitigation and resolution of the breach of security or loss of integrity.

5. The notification referred to in the preceding paragraph is to include the following information:

a) Name, telephone number and email address of a representative of the undertaking for the purpose of any contact by ICP-ANACOM;
b) Date and time that the breach of security or loss of integrity took on significant impact or, where this cannot be determined, the date and time of its detection;
c) Date and time that the breach of security or loss of integrity ceased to have significant impact or, where impact persists, the date and time that it is estimated that significant impact will cease;

d) Brief description of the security breach or loss of integrity, including an indication of the category of the root cause and, as far as possible, the details;

e) Possible estimate of its impact in terms of:

   i) networks and services affected;

   ii) access to emergency services;

   iii) number of subscribers or accesses affected;

   iv) geographical area affected, in km^2; and

f) Observations.

6. After the breach of security or loss of integrity ceases to have significant impact, and whenever it has not already been reported in the initial notification, undertakings are required submit to ICP-ANACOM, at the earliest opportunity and within a maximum period of two hours after such impact ceases, notice that the breach of security or loss of integrity with significant impact has been resolved.

7. The notification referred to in the preceding paragraph must, as far as possible, include the following information:

a) An update to the information provided in the initial notification; and

b) A brief description of actions taken to resolve the breach of security or loss of integrity.

8. The final notification is to be sent within a period of twenty working days from the time that breach of security or loss of integrity ceases to have significant impact.

9. The notification referred to in the preceding paragraph must include the following information:

a) Date and time that the breach of security or loss of integrity took on significant impact or, where this cannot be determined, its detection;

b) Date and time that the breach of security or loss of integrity ceased to have significant impact;

c) Date and time that the security breach or loss of integrity commenced, or where this is not possible to determine, the date and time of its detection and date and time of cessation, where different from the dates and hours reported, respectively, in accordance with points a) and b);

d) Impact of the breach of security or loss of integrity in terms of:

   i) Networks (including national and international interconnections) and respective infrastructure (including systems) and affected services;

   ii) Access to emergency services using 112 (single European emergency number) (including access using the national emergency number 115);

   iii) Number of affected subscribers or accesses by network or service;

   iv) Percentage of affected subscribers or accesses as proportion of total subscribers or accesses by network or service access; and

   v) Geographical area affected, in km^2;

e) Description of the security breach or loss of integrity, including indication of the category of the root cause and detail;

f) Indication of measures taken to mitigate the breach of security or loss of integrity;

g) Indication of measures adopted to resolve the breach of security or loss of integrity, including, in the event of breaches of security or loss of integrity with partial restoration, the chronology and detail of the stages of restoration;

h) Indication of the measures taken and/or planned to prevent or minimize the occurrence of similar security breaches or losses of integrity in the future (in terms of planning and/or operations, of contingency planning, of interconnection agreements, of service level agreements and other relevant areas) and the date on which they took or will take effect;

i) When appropriate, the information made available to the public regarding the breach of security or loss of integrity, including any updates to this information, and the date and time of such disclosure;

j) Other relevant information; and

k) Observations.

10. For the purposes of paragraphs 5, 7 and 9 of this Section II, the root causes of breaches of security or loss of integrity can have the following categories:

a) Accident/natural disaster;

b) Human error;

c) Malicious attack;

d) Hardware/software failure; or

e) Failure by an external party to supply goods or services.

11. Wherever possible, the information included in the notifications set out in the present Section II on the number of subscribers or accesses is to follow the definitions set out in the framework of obligations governing the periodic submission of information to ICP-ANACOM.

12. The notifications set out in the present Section II are to be performed using the following means:

a) as regards initial notifications and notifications of cessation of breaches of security or losses of integrity with significant impact, by email to notifica@anacom.pt and by telephone 214340899; and

b) as regards the final notification, by delivery in person or by registered mail.

13. Companies whose networks or services have their functioning impacted by such breaches of security or losses of integrity are to cooperate among themselves to ensure the proper detection of any breach of security or loss of integrity and to undertake assessment of its impact, and in the case referred to in point g) of paragraph 3 of Section I, for the respective notification.

14. With a view to the proper performance of the provisions of the present Annex A, it is incumbent upon the undertakings to deploy all the resources and procedures as are necessary to detect and evaluate security breaches or losses of integrity covered by the circumstances set out in Section I, assess their respective impact and undertake notification.

III. Entry into force and transitional provision

1. The undertakings are required to implement such measures as are necessary in order to comply with the provisions of the present Annex A, doing so no later than 12 June 2014, without prejudice to the following paragraph.

2. Based on available data and with reference to the circumstances described in Section I of the present Annex A and the requirements for the final notification given in paragraph 9 of Section II, undertakings are required to submit to ICP-ANACOM:

a) a report on the period starting on 1 January 2013 and ending on the date of approval of the present decision, which report is to be submitted no later than 12 January 2014; and

b) six monthly reports, covering the entire period specified in paragraph 1 of the present Section III, each report to be submitted no later than one month following the end of the period to which it relates.

ANNEX B to the Draft Decision

- **Cabovisão** believes that there is no legal basis for the obligation imposed by ICP-ANACOM, and deems it disproportionate, proposing that if ICP-ANACOM maintains the provisions of the draft decision, it should set the thresholds at less demanding levels.

  It considers the requirement for disclosure on the website of the company for a period of 6 months to be excessive, and considers the telephone contact covering the IVR, as well as the proposed deadline (which should be 2 days) to be sufficient.

  Reaffirming its opposition in principle to the matter, it holds that a minimum period of six months should be considered for implementation.
- **CTT** considers that disclosure to a broad public not seeking the information could give rise to a certain *"alarmism"*, whereby the usefulness of this measure needs to be assessed, and that ICP-ANACOM should follow international practice of determining which security incidents to disclose on a case-by-case basis.

  It considers that disclosure should be limited to a contact given for members of the public seeking information and holds that it would be reasonable to have information available for a period of one (1) month.

  Finally CTT considers the period of 30 days given for entry into force to be unworkable
- **Grupo ONI** believes that public disclosure could cause situations of *"alarmism"* and potentially malicious attacks due to the disclosure of vulnerabilities; disclosure should therefore be limited to minimize additional risks.

  It disagrees with the maintenance of history on the company *websites*, and suggests periods of disclosure of 48 hours following determination by ICP-ANACOM.

  If the provisions of the draft decision are maintained, it holds that the information on the *website* should be maintained for 5 days, and that entry into force and the period of the transitional provision should be extended, respectively, to 6 and 5 months.
- **Optimus** also refers to the possibility that, by revealing network vulnerabilities or failures, this measure may cause more harm than good.

  Optimus considers the period of one hour to be unrealistic, suggesting 4 working hours following detection of a security incident and the determination of the regulator and its proper notification to the company.

It does not agree with publication on line, and in particular, maintenance of the information online for 6 months, and considers that the information available should provide clarification but with an appropriate degree of detail according to a cost/benefit analysis in each situation.

It makes a proposal based on the table already transposed above, with disclosure after 4 working hours and only following a decision by ICP-ANACOM.

The implementation period should be at least 6 months.

- **Grupo PT** states that *"in order to avoid a climate of widespread distrust of operators, notification of customers should be imposed only when precisely, there is a real risk of the incident causing damage and when such notification entails a real advantage for customers"*.

  The company considers that operators should be allowed some leeway or it should be established that only serious incidents affecting 112 should be covered.

  It calls for clarification regarding the requirement for a specific telephone number and holds that the means of contact should be determined on a case-by-case basis according to the type of incident and its level of criticality.

  It takes the view that the deadline for disclosure of information to the public is *"very demanding"*, and that the maintenance of the disclosure on the *website* for 6 months is *"absolutely excessive"*.

  Finally, the group considers that entry into force and the period of the transitional measure should be at least 6 months.

- **VodafoneS.I.C. [Start of Confidential Information]**

  E.I.C. [End of Confidential Information]

- **APRITEL** believes that, ultimately, only *"certain serious incidents, affecting access to 112, should be covered by a prior determination of public interest"*.

  APRITEL also refers to possible *unnecessary "alarmism"* and that *"there may be customers who are notified of situations relating to services that they do not even use or which they only use on a very occasional basis"*, whereby the practice *"may also contribute to undermining public trust in communications services"*.

  The Association also cites issues stemming from the exposure of vulnerabilities, that the indication of expected problem resolution time may *"fuel situations of abuse by customers"*, and that the deadline for disclosure is unrealistic.

  It considers that the decision should enter into force following a period of 6 months.

- **GRM**, given the specificities of the Autonomous Regions, considers that security incidents referred to in item iv. of point c) of paragraph I of Annex A to the draft decision should also be subject to public disclosure .

  On the other hand, it considers that *"cyber-attacks which impact government companies or agencies"* should not be subject to public disclosure.

POSITION OF ICP-ANACOM

Below, we present the reasoning that supports the final version of Annex B, highlighting, above all and essentially, the following amendments:

- Elimination of the thresholds of lesser impact as regards the number of subscribers or accesses affected (or affected geographic area);
- Elimination of the obligation to provide a contact telephone number;
- Deadline for disclosure in working hours; and
- Extension of entry into force to a period equal to six months.

1. Firstly it should be clarified and highlighted that the conditions originally set out in draft decision as regards the obligation of public disclosure of breaches of security or losses of integrity are related solely to the circumstances provided for in the prior paragraph a) of Section I of Annex A of the draft decision, not covering, therefore, any of the other points in this Section.
2. Note is made of the provisions which, on this issue, are included in chapter 3 of the regulation of the Finnish NRA, FICORA, and which are somewhat in line with our view.
3. Both Grupo PT and APRITEL raise the possibility of only making public disclosure of information as to security incidents involving 112 service call centres;

   ICP-ANACOM considers that, in this particular case, ICP-ANACOM should assess the situation if and when this happens, because from the outset it should be noted that 112 call centres are the responsibility of the Ministry of Internal Affairs.
4. Contrary to the cited potential *"alarmism"* and *"undermining of public trust in communications services"* ICP-ANACOM, beyond what has been set out above, takes the following position:
   a. One of the rationales of the Framework Directive and of the LCE as regards security and integrity of networks and services is, as already mentioned above, transparency;
   b. Potential *"alarmism"*, *or "undermining of trust"*, or even speculation, might arise from the disclosure to the public of unreliable information, not properly handled by the party who has it at first hand and who therefore has the opportunity and the duty to properly inform the public;
   c. Obviously, it will not be, in principle, in the public's interest to have knowledge of any vulnerabilities that may or have been exploited, and this has never been *"on the table"*;
   d. We believe that it is in the public's interest to have information, at the earliest opportunity, when a security incident occurs with significant impact on users and, which nowadays cannot be concealed; it is, in our view, less alarmist, less speculative, and

more positive in terms of the image of the companies, where the companies themselves provide the information in good time about such security incidents;

5. Furthermore, and contrary to what has been reported by several companies, information about a particular security incident is not, in the majority of cases, of interest merely to the subscribers directly affected, but also to all other users who are then prevented from communicating with these subscribers.
6. As regards the disclosure of security incidents occurring in Autonomous Regions, in accordance with the provisions of item iv) of point c) of Section I of Annex A of the draft decision, it is considered that it would be disproportionate, and is subject to analysis by ICP-ANACOM upon any occurrence.
7. As regards safeguarding public disclosure of *"cyber-attacks that impact government companies or agencies"*, it is stated that, from the outset, that the objective is not to release information to the public, in the context of the present question, as regards security incidents impacting this or that particular end-user.
8. Having considered the comments received as to establishing the size of the impact of security breaches or losses of integrity in determining their public disclosure, it is considered that, at this time, only security breaches or losses of integrity with greater impact should be considered, whereby, under the terms defined in paragraphs 2 and 3 Section I of Annex B, the two lowest thresholds, in terms of number of subscribers or accesses affected (or affected geographic area), as previously included in the draft decision, are eliminated.
9. In addition, and for purposes of interpretation and application of the circumstances referred to in paragraph 2 of Section I of Annex B, rules which are identical to those set out in paragraph 4 of Section I of Annex A are transposed to paragraph 3 of this Section.
10. As regards the content of the information to be made available, companies must have appropriate communication procedures that do not jeopardise the security of their networks and services;

    The content of information to be disclosed about security breaches or

losses of integrity must be, as is mentioned in point a) of paragraph 1 of Section II of Annex B, clear, accessible and as precise as possible, and must include, among other elements considered relevant, indication of the networks and services affected and the expected time to be taken for resolution or, if applicable, the date of resolution.

With regard to deadlines, APRITEL's concern about disclosure of likely time to be taken for resolution *"as fuelling situations of abuse by customers"* is not understood; as they do not expound, and recalling that the public will not, in principle, be aware of any security incidents that do not impact the normal functioning of networks and services in a manner perceptible to the user, the scope of what APRITEL referred to is not understood.

11. The means by which companies must provide information to the public should, at a minimum, entail the websites that they use in their dealings with the users of their networks and their services, through an immediately visible and identifiable link on their homepage, visible without needing to use the website's scrollbars, in accordance with point b) of paragraph 1 of Section II of Annex B.

    At this point and contrary to what we anticipated in the draft decision, and contrary to what was adopted by FICORA, the position is now taken that a specific telephone number should not be used for the public to obtain information about a specific security incident, as this is not the most appropriate means of disclosing information; however it is considered that, where contacted about the occurrence through this channel, companies must continue to keep their subscribers duly informed about security incidents affecting them, according to the general duties of information resulting from the law, from contracts and from the principle of good faith.

12. On the other hand we were sensitive to some arguments put by respondents, such as timetable over 24 hours, or about the cost of the work or as to the importance of disclosing information (and that this can always be amended if, in specific cases, ICP- ANACOM so determines), and the need for more time to process information so that this can be informative, and so:

a. ICP-ANACOM considers that, as is now set out in point c) of paragraph 1 of Section Point II of Annex B, the information should be disclosed as soon as possible, within four working hours following the deadline of initial notification to ICP-ANACOM of a security breach or loss of integrity set out in Section II of Annex A, considering as working hours, for this purpose, the time elapsing between 9 am and 7 pm on a working day;
b. For example, if the deadline for initial notification to ICP-ANACOM of a breach of security or loss of integrity finishes at 10pm on a given day, the information regarding the incident is to be made available to the public by no later than 1 pm on the following working day;
c. In accordance with point d) and e) of the same paragraph 1 of Section II of Annex B, the companies are required to update the information whenever there is a significant change and directly following cessation of the breach of security or loss of integrity; the companies are also required to maintain the information made available over the Internet accessible to the public for a period of one month from the date of the cessation of the breach of security or loss of integrity, in line with what has been adopted by FICORA.

13. Under paragraph 2 of Section II of Annex B, companies are required to communicate, at the beginning of their activity or when amending them, the URL addresses of their websites where, for the purposes of point b) of paragraph 1, information is provided to the public.
14. In accordance with the provisions of the new paragraph 3 of Section II of Annex B and in order to fully comply with the provisions of this Annex B, it is determined that it is incumbent upon the undertakings to implement all the means and procedures as are necessary to detect and evaluate security breaches or losses of integrity covered by the circumstances set out in Section I of the same Annex B.
15. For the reasons mentioned above and under the terms that are set out in paragraph 1 of Section III of Annex B, ICP-ANACOM considers that

the deadline for entry into force shall correspond to a period of six months following the date of the final decision. In order that ICP-ANACOM is, from the outset, equipped with the information it needs to monitor implementation of this decision, it is further set out in paragraph 2 of the same Section III that, within a minimum of 15 working days following expiry of the period provided for entry into force, the companies are required to notify ICP-ANACOM as to the URL addresses of the pages where information relating to breaches of security or losses of integrity will be made available to the public.

16. As performed with respect to Annex A of the decision, Annex B is reformulated in order to provide greater precision and clarity.

FINAL VERSION OF THE ANNEX B

Public disclosure, by undertakings that provide public communications networks or publicly available electronic communication services, of security breaches or losses of integrity occurring on their networks and services

I. Conditions

1. Pursuant to point b) of article 54-E of Law no. 5/2004 of 10 February, as amended and republished by Law no. 51/2011 of 13 September (hereinafter "Electronic Communications Law"), it is incumbent upon ICP - Autoridade Nacional de Comunicações (ICP-ANACOM) to require undertakings which provide public communications networks or electronic communications services accessible to the public (hereinafter, the "undertakings") to inform the public, by appropriate means, of breaches of security or losses of network integrity, where deemed by ICP-ANACOM as being in the public interest.

2. ICP-ANACOM determines that it is in the public interest that undertakings inform the public as to any breach of security or loss of integrity whose impact on the functioning of their networks and services is encompassed by the following criteria:

Duration and	**Number of subscribers or accesses affected** **(or, pursuant to point e) of paragraph 3 of Section I, geographic area affected)**
≥ 30 minutes	no. of subscribers or accesses affected ≥ 500,000 (or, pursuant to point e) of paragraph 3 of Section I, geographic area affected - 3,000 km^2)
≥ 1 hour	500.000 > number of affected subscribers or accesses ≥ 100,000 (or, pursuant to point e) of paragraph 3 of Section I, 3,000 km^2 > geographic area affected ≥ 2,000 km^2)
≥ 2 hours	100.000 > number of affected subscribers or accesses ≥ 30,000 (or, pursuant to point e) of paragraph 3 of Section I, 2,000 km^2 > geographic area affected ≥ 1,500 km^2)
≥ 4 hours	30.000 > number of affected subscribers or accesses ≥ 10,000 (or, pursuant to point e) of paragraph 3 of Section I, 1,500 km^2 > geographic area affected ≥ 1,000 km^2)

3. For the purposes of the preceding paragraph:

a) The impact of a breach of security or loss of integrity is to be assessed by reference to all the networks and all the services of a company that are affected thereby;
b) The number of subscribers or accesses affected by a breach of security or loss of integrity corresponds to the sum of the number of subscribers or accesses which are so affected and as comprised by the various networks and services;
c) The number of subscribers to a service that is supported by another service will only be taken into account when the support is not affected;
d) The number of subscribers or accesses affected corresponds to the number of subscribers or accesses covered by the breach of security or loss of integrity, or where it is not possible to determine this number, to an estimate based on statistical data held by the undertaking; and
e) The criterion related to the affected geographical area is only to be applied in the event that the criterion on the number of affected subscribers or accesses is inapplicable or, in the specific case and on a reasoned basis, impossible to determine or estimate.

4. Notwithstanding the provisions of the present Annex B, ICP-ANACOM may, pursuant to paragraph b) of article 54 of the Electronic Communications Law, including in circumstances not provided for in paragraph 2 of the present Section I, order undertakings to inform the public as to other breaches of security or losses of integrity occurring on their networks and as part of their services.

II. Contents, means and timing of disclosure

1. In their disclosure to the public of breaches of security or losses of integrity referred to in Section I, undertakings are required to:

a) Ensure that the content of the disclosure is clear, accessible and as precise as possible and includes, among other relevant information:

i) Indication of the networks and services affected; and

ii) The length of time it is expected to take to resolve the occurrence or, if applicable, the date of resolution;

b) Provide, as a minimum, information on their respective web sites, as used in their relationship with users, through a hyperlink posted on the homepage of the website, which hyperlink shall be immediately visible and identifiable without scrolling;

c) Provide the information at the earliest opportunity and within four business hours following the deadline of the initial notification to ICP-ANACOM[23],for this purpose, working hours means time elapsing between 09.00 and 19.00 on a working day;

d) Update the information whenever a significant alteration occurs and immediately after the breach of security or loss of integrity ceases; and

e) Ensure that the information provided on the Internet remains accessible to the public, in the same locations as referred to in point b), for a period of one month following the date on which the breach of security or loss of integrity ceases.

2. Companies are required to notify ICP-ANACOM, upon commencing their activity, as to the URL addresses[24] of web pages which, for the purposes of point b) above, they will use to provide public disclosure of security breaches or losses of integrity occurring on their networks and as part of their services, and notify ICP-ANACOM as to any subsequent amendments thereto within a minimum of 5 working days subsequent to such amendments being implemented.

3. With a view to the proper performance of the provisions of this Annex A, it is incumbent upon the undertakings to implement all the means and procedures as are necessary to detect and evaluate security breaches or losses of integrity covered by the circumstances set out in Section I, assess their respective impact and undertake notification.

III. Entry into force and transitional provision

1. The undertakings are required to implement such measures as necessary in order to comply with the provisions of the present Annex B, doing so no later than 12 June 2014.

2. Undertakings are required to notify ICP-ANACOM, a minimum of 15 working days prior to the expiry of the period specified in the preceding paragraph, as to the URL addresses referred to in paragraph 2 of Section II.

---

[23] In accordance with the provisions of Section II of Annex A.

[24] Uniform Resource Locator.